UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/556,068	04/21/2000	Sai V. Allavarpu	5181-48400	6894

58467 7590 06/09/2008
MHKKG/SUN
P.O. BOX 398
AUSTIN, TX 78767

EXAMINER
PATEL, HARESH N

ART UNIT	PAPER NUMBER
2154	

MAIL DATE	DELIVERY MODE
06/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/556,068	**Applicant(s)** ALLAVARPU ET AL.	
	Examiner Haresh N. Patel	**Art Unit** 2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☒ Claim(s) *61-63* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-63 are subject to examination. Claims 61-63 are allowed.

2. As per the appeal review, paper dated 4/1/2008, the finality of office action, dated 11/28/2007, is withdrawn and the prosecution is hereby reopened. Further search regarding the applicant's concerned "**object level access control**" in fact revealed additional **multiple evidences** to support that "**object level access control**" as claimed was not only published by several **assignees but also by the assignee of this application, SUN Microsystems**, at least more than one year prior to the filling date of this application (1997). (Please refer to the below rejections containing the evidences, for example, "Sun Launches New Version of its High-End Network Management Software", pages 1-6, Nov. 11, 1997", contains following statements among other citations of the object level: Solstice Enterprise Manager is unique in that it provides the **distributed** multi-protocol management solution that can **manage networks with millions of objects** and ever-changing technologies, and enables providers to be first to market with differentiated services marked by visible quality. Solstice Enterprise Manager 2.1: -0- -- Builds on the power of the product's scalable and **distributed architecture,** by breaking out common management services into **distributed components**. For the first time, customers can distribute the logging, Simple Network Management Protocol, Common Management Information Protocol and Remote Procedure Call services as **separate processes in the network**. -- Liberates network administrators by allowing them to provide customers with **highly-secured access** to management information through new **object-level access control**. For example, an IT organization responsible for discreetly managing services available within both

the engineering and finance organizations should keep these separate domains with **rights, privileges and access very carefully controlled**. **Secure management functionality** is built into Solstice Enterprise Manager. This can also be used by **ISPs spanning** commerce efforts across **multiple companies** (e.g., network management service provided to both Coke and Pepsi, etc.,). This office action is made non-final with the rejections including this available evidence. Also, the applicant's statements, see office action dated 6/18/2007, since **a firewall device** coupled between a home PC and the Internet implies **the firewall device would unable to prevent** a malicious PC from interfacing with the home PC, are considered for the rejections. Further, Cover Pages: XML Articles and Papers. January-March 2000, pages 1-111, 3/31/2000, Containing at least: **Microsoft, Novell, Sun,** and others must speak the same language. The Directory Services Markup Language (DSML) might just be the key. This month Rawn Shah reviews DSML. "Although there have been numerous directory services products over the years, Microsoft's recent release of Active Directory, which is bundled with Windows 2000, promises to make itself mandatory in medium- to large-scale Windows-centric networks. It may not be the most versatile system in the world, but it can improve the management of hundreds or thousands of Windows desktops and servers. Although Active Directory implements version 3 of the Lightweight Directory Access Protocol (LDAP), it also extends it and adds some Windows specific features. Microsoft isn't alone in adding to LDAPv3, which does have its limitations. For example, Novell's NetWare Directory Services (NDS) also enhances the LDAPv3 protocol to add their own features. One important missing feature is **object-level access control**. Each entry object in the directory should have its own access control list that indicates which users are allowed access to the data contents of the entry and which aren't. Both NDS and Active Directory have this, albeit in different forms. Such enhancements alter the way directory entries may be accessed from an application, thus making, for example, a NetWare-based application incompatible with some of the data stored in Active Directory. . . . Like XML, DSML has platform-independent syntax that can be implemented on practically any platform available today. It separates the contextspecific semantics of the document contents from the platform-specific semantics, which makes an entry in one directory understood as an entry in all directories. Some entries may have additional attributes that others don't, so DSML provides a way to translate an entry from one directory format to another. Each directory accepts the attributes it can store and creates default values or queries for additional information on missing entries. DSML is language that describes the structure of directories (schema), and the contents of directory entries. In other words, it's a structured form that describes another structured form. Because both directories and XML commonly use terms such as attributes, schema, objects, etc., it's important to distinguish the difference when talking about DSML. A directory schema thus refers to the structure of the data elements contained within the directory, as opposed to the DSML schema that refers to the ruleset of how to translate between directories..." See "Directory Services Markup Language (DSML)."

[March 31, 2000] "Increase Web-Page Performance with Server-Side XSL." By Paul Enfield. MSDN Online Magazine. April, 2000. ['This MSDN Magazine article shows how to boost performance and reduce database load by using server-side XSL to generate datadriven Web pages in advance of page requests. Dynamic data-driven pages have become the basis of many cutting-edge Web sites. Early render systems can provide better performance and maintainability for data-driven Web sites by generating frequently accessed pages that contain less-volatile information ahead of time. We'll show you an example of a server-side solution that uses Extensible Stylesheet Language (XSL) to merge data and layout information into HTML that is compatible with just about any modern Web browser. Using these techniques to render Web pages early can reduce the load on your database back end and increase performance for your users.'] "Web content has evolved from primarily static information to data-driven pages and now to dynamic database, etc.

Patent 6,405,202, also containing other citations of the object level with at least: Current object level access controls regulate user access to each object individually, however requiring additional overhead. As specialization continues to increase with system complexity, individual professionals will access only selected domains of information, some of which will span subsets of multiple objects. For example, a network engineer may require access to electrical and performance domains as well as relationships specifying interconnections, but not necessarily to cost information. Therefore, there is a need to control access at the domain level. Since domains consist of a group of one or more properties and domains can overlap, there is a need to efficiently control access at the property level. There is also a need for improved_object level access control_for cases where an object contains properties that cover multiple domains. OODB vendors, for example, Versant Corp., Object Design, Computer Associates, GemStone Systems, Inc. and Ardent Software, Inc. have not provided this level of access control or security. Accordingly, there is a need for property level access control that can be implemented in a flexible and efficient manner, etc.

Double Patenting

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or anticipated by, the earlier claim".

In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Bern, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousness-type double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

3. Claims 1-6, 8-11, 16, 17, 20-25, 27-30, 35, 36, 39-44, 46-49, 54, 55, 58-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-39 of copending application, 09/552,984, now patent number 7,010,586, as per the office action dated 10/5/2006. For further clarification, the applicant's concerned "**object level access control**" in fact revealed **multiple evidences** that "**object level access control**" as claimed was not only published by several **assignees but also by the assignee of this application, SUN Microsystems**, more than one year prior to the filling date of this application, and regarding the applicant's further concerns of the double patenting rejection, below is the claims of the copending application, with emphasis as per the applicant's request for the concerned limitations, (claim 1) a network management system comprising: **an event gateway**

which is coupled to **one or more managed objects and which is configured to deliver events generated by the managed objects to one or more managers**, and **a plat form-independent interface to the event gateway**, wherein the event gateway is configurable to communicate with the managers through the platform- independent interface to **deliver the events generated by the managed objects**; wherein the event gateway comprises **a plurality of event distribution server sinks configured to receive events generated by file managed objects and to distribute the events to fine one or more managers such that one of the managers receives events from a plurality of' different ones** of the event distribution server sinks; and wherein the gateway is configurable to provide the mangers with subscriptions to the events as a function of event criteria specified by the managers, whereby events meeting the specified event criteria are delivered and events filtering to meet the specified event criteria are filtered out. Claim 2. The network management system of claim 1, wherein the **event criteria** comprise an object class for the managed objects generating file events. 3. The network management system of claim i, wherein the event criteria comprise an object instance **for one of the managed objects generating the events**. 4. The network management system of claim 1, wherein the event criteria comprise **an event type**. .5. The network management system of claim 1, wherein the platform- independent interface to the event gateway is expressed in an **interface definition language**, and wherein the interface definition language comprises a language for defining interfaces to managed objects across a plurality of platforms and **across a plurality of programming languages**. 6. The network management system of claim 5, wherein the interface definition language comprises **Object Management Group Interface Definition Language (OMG IDU) interface**. 7. The network management system of claim 1, wherein the managed objects comprise one or morn objects corresponding to **a telephone network**. 8. The network management system of claim 1, wherein fine managed objects comprise an object corresponding to a **telecommunications** device. 9. The network management system of claim 1, wherein the event gateway comprises: **an event distribution server, wherein the event distribution server is configurable to listen for the events generated by the one or more managed objects and deliver the events to the one or more managers**, wherein the event distribution server comprises the plurality of event distribution server sinks. 10. The network management system of claim 9, wherein the event gateway further comprises: an event port registry server comprising a plurality of event ports and an **event port registry, wherein the server is coupled to the event distribution server, wherein the event ports comprise communication channels for the delivery of the events to the one or more managers**, and wherein the event port registry provides information to the event distribution server regarding which ports correspond to which managers. 11. The network management system of claim 9, wherein the event distribution server comprises: an event **distribution server source which listens for the events from the one or more managed objects', and wherein the plurality of event distribution server sinks are operable to dispatch the events to the one or more managers as a of the subscriptions**. 12. The network management system of claim 11, wherein the event distribution server sinks are distributed to provide **load balancing of the events to the one or more managers**. 13. The network management system of claim 1, wherein the events are delivered through the platform-independent interlace according to Internet Inter- Object Protocol (**IIOP**).

4. Claims 1-6, 8-11, 16, 17, 20-25, 27-30, 35, 36, 39-44, 46-49, 54, 55, 58-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-44 of U.S. Patent, 6839748, as per the office action dated 10/5/2006.

5. For further clarification, the applicant's concerned "**object level access control**" in fact revealed **multiple evidences** that "**object level access control**" as claimed was not only published by several **assignees but also by the assignee of this application, SUN Microsystems**, more than one year prior to the filling date of this application, and regarding the applicant's further concerns of the double patenting rejection, below is the claims of the copending application, with emphasis as per the applicant's request for the concerned limitations,

Claim 1. A **network management system** comprising: **a gateway which is coupled to one or more managed objects and which is configured to deliver messages between the managed objects and one or more managers; a platform-independent interface to the gateway, wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the messages; a thread pool which provides allocation of thread resources to each of the one or more managers;** and one or more synchronous task schedulers corresponding respectively to **each of the managers, wherein each synchronous task scheduler is operable to receive and enqueue pending messages associated with the corresponding manager and to dequeue and deliver each of the pending messages using a thread from the thread pool upon completion of delivery of previous messages** so that the messages are delivered in an order in which the messages were enqueued. 2. The network management system of claim 1, wherein the messages are communicated with the manager via Internet Inter-Object Protocol (IIOP). 3. The network management system of claim 1, wherein the **platform-independent interface to the gateway is expressed in an interface definition language**, and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages. 4. The network management system of claim 3, wherein **the interface definition language comprises OMG IDL**. 5. The network management system of claim 1, wherein the managed objects comprise one or more objects corresponding to a telephone network. 6. The network management system of claim 1, wherein the managed objects comprise an object corresponding to a **telecommunications** device. 7. The network management system of claim 1, wherein the gateway comprises **an event gateway, and wherein the messages comprise events associated with the managed objects**. 8. The network management system of claim 1, wherein the gateway comprises a request gateway which is configured to **deliver messages generated by one or more managers to the one or more managed objects**, and wherein the messages comprise requests for the one or more managed objects. 9. The network management system of claim 8, wherein the **requests comprise a query for information concerning one of the managed objects**. 10. The network management system of claim 8, wherein **the requests comprise a command to set one or more parameters of one of the managed objects. 11. The network management system of claim 8, wherein the requests are converted from the**

interface definition language to a Portable Management Interface (PMI) format prior to delivery to the managed objects. 12. The network management system of claim 8, wherein the requests are converted from the interface definition language to a platform-specific format prior to delivery to the managed objects. 13. The network management system of claim 1, wherein the gateway comprises an event gateway, and wherein the messages comprise events associated with the managed objects. 14. The network management system of claim 13, the events comprise an alert generated by one of the managed objects.

6. Claims 1-6, 8-11, 16, 17, 20-25, 27-30, 35, 36, 39-44, 46-49, 54, 55, 58-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-30 of U.S. Patent, 6813770, as per the office action dated 10/5/2006.

7. For further clarification, the applicant's concerned "**object level access control**" in fact revealed **multiple evidences** that "**object level access control**" as claimed was not only published by several **assignees but also by the assignee of this application, SUN Microsystems**, more than one year prior to the filling date of this application, and regarding the applicant's further concerns of the double patenting rejection, below is the claims of the copending application, with emphasis as per the applicant's request for the concerned limitations,

1. A network management system comprising: a plurality of plug-in mapping modules, wherein each of the plurality of plug-in mapping modules is operable to provide a unique mapping for a set of managed object data types between the same two languages for describing data associated with managed objects, wherein

one of the two languages is an interface definition language (IDL) and the other of the two languages is an abstract syntax notation, wherein the interface definition language comprises a language for defining interfaces to managed objects across a plurality of platforms and across a plurality of programming languages, wherein the managed objects comprise instances of the managed object data types, **and wherein the abstract syntax notation comprises a language for describing data; and a mapping framework, wherein the mapping framework is operable to receive the plurality of plug-in mapping modules, and wherein the mapping framework is operable to provide access to the plurality of plug-in mapping modules to facilitate the mapping of managed object data types in accordance with the mappings for managed object data types provided by the plurality of mapping modules.** 2. The system of claim 1, wherein the managed objects comprise a telephone system. 3. The system of claim 1, wherein the managed objects comprise a network switch. 4. The system of claim 1, wherein the mapping framework comprises a plurality of processes which are concurrently executable. 5. The system of claim 1, wherein **the interface definition language is operable to provide a single mapping which is applicable to any managed object class.** 6. The system of claim 1, wherein the abstract syntax notation comprises Abstract Syntax Notation One (ASN1). 7. The system of claim 1, wherein the mapping framework comprises **a converter framework library, wherein the converter framework library comprises a set of abstract classes which provide an interface for the one or more plug-in mapping modules, and wherein the interface comprises wrappers to a plurality of corresponding converter implementation classes;** and wherein a converter implementation library comprises the one or more plug-in mapping modules, wherein the one or more **plug-in mapping modules comprise the plurality of converter implementation classes, and wherein the converter implementation classes provide mappings for the managed object data types between the interface definition language and the abstract syntax notation**. 8. The system of claim 7, wherein the **converter framework library comprises an ASN1 converter framework library, and wherein the ASN1 converter framework library provides an interface to map managed object data types between ASN1** and the interface definition language. 9. The system of claim 7, wherein **the converter implementation library comprises a C++ IDL to ASN1 converter implementation library, and wherein the C++ IDL to ASN1 converter implementation library comprises C++ classes and functions to map managed object data types between ASN1 and the interface definition language.** 10. The system of claim 7, wherein the converter framework library comprises a collection of classes, and wherein the classes comprise wrappers to corresponding implementation classes in the converter implementation library.

8. Claims 1-6, 8-11, 16, 17, 20-25, 27-30, 35, 36, 39-44, 46-49, 54, 55, 58-60 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-34 of U.S. Patent, 6950935, as per the office action dated 10/5/2006.

Note: The applicant's arguments regarding the double-patenting rejections are considered and hence the claims for the double patenting rejection are updated.

9. For further clarification, the applicant's concerned "**object level access control**" in fact revealed **multiple evidences** that "**object level access control**" as claimed was not only published by several **assignees but also by the assignee of this application, SUN Microsystems**, more than one year prior to the filling date of this application, and regarding the applicant's further concerns of the double patenting rejection, below is the claims of the copending application, with emphasis as per the applicant's request for the concerned limitations,

Claim 1: **A network management system** comprising: a client-side authentication library deployed on one or more client computer systems, wherein the client-side authentication library comprises a client-side interface which is operable to retrieve and encrypt **a user profile associated with a user, and wherein the client-side library is implemented in accordance with a platform-independent interface specification and implemented for one or more client platforms respectively corresponding to each of the one or more client computer systems; and a server-side authentication library deployed on a server computer system coupled to the client computer system, wherein the server-side authentication library comprises a server-side interface which is operable to receive the encrypted user profile from the client-side authentication library and decrypt the user profile to authenticate the user for one or more network services, and wherein the server-side library is implemented in accordance with the platform-independent interface specification and implemented for a server platform corresponding to the server computer system**. 2. The network management system of claim 1, wherein the client-side authentication library is shared **by a plurality of management applications**. 3.

The network management system of claim 1, wherein the server-side authentication library is shared **by a plurality of gateway components.** 4. The network management system of claim 1, wherein the server-side **authentication library is implemented in C++**. 5. The network management system of claim 1, wherein **the user profile comprises a user name and a password. 6. The network management system of claim 5, wherein the user profile further comprises a designation of a management information server (MIS) to which the user wishes to connect.** 7. The network management system of claim 1, wherein the platform-independent interface specification comprises a **specification expressed in an interface definition language (IDL), wherein the interface definition language is operable to define object interfaces across a plurality of platforms and across a plurality of programming languages. 8. The network management system of claim 1, wherein the user profile is encrypted and decrypted according to a user-selected encryption scheme**. 9. The network management system of claim 1, wherein the client-side authentication library and the server-side authentication library are operable to authenticate requests received by **a CORBA gateway, wherein** the requests comprise management requests to one or more managed objects, and wherein the management requests are **sent by one or more manager applications**.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 5-7, 9, 16-17, 20, 24-26, 28, 35-36, 39, 43-45, 47, 54-55, 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent et al. U.S. patent number 6,363,421, Lucent Technologies (Hereinafter Barker-Lucent) in view of "Sun Launches New Version of its High-End Network Management Software", pages 1-6, Nov. 11, 1997" (Hereinafter SUN).

12. As per claims 1, 20, 39, 58-60, Barker-Lucent teaches the following:

a network management method / a carrier medium/ system comprising (e.g., col. 1, lines 27-30),

a gateway (e.g., an element management server, col.1, lines 27-30) which is coupled to a plurality of managed objects (e.g. col. 1, lines 29-36) and which is configured to deliver events generated by the managed objects to manager (e.g., col. 1, lines 63-65) or to deliver requests generated by the managers to the managed object (e.g., col. 1, lines 63-65); and

a platform-independent interface to the gateway (e.g., col. 4, lines 37-55), wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the events or requests (e.g., col. 1, lines 63-65),

wherein the gateway is configurable to provide object-level control (e.g., usage of a col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63), between the managers (e.g., col., 8, line 53 – col., 9, line 19) and the managed objects (e.g., col., 8, line 53 – col., 9, line 19) to send the requests to the managed objects (e.g., col., 8, line 53 – col., 9, line 19),

sending an identity of a user of a manager application to a gateway (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63), determine on a managed object level whether or not the manager application (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63) is allowed to receive an event generated by one of plurality of managed objects (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63) or to send a request to the one of the plurality of managed objects (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63) as a function of the identity of the user of the manager application (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63), whereby access for the manager application to send the request is approved or denied for said managed object (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63).

delivering the event to the manager application or the request to the managed object if the manager access is approved (e.g., col., 8, line 53 – col., 9, line 19, col., 7, lines 47 – 63).

However, Barker-Lucent does not specifically mention about individual object level.

SUN discloses the well-known concept of usage at individual object level, access control so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects access control so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects and the usage of a request Service Access Point (SAP), "Sun Launches New Version of its High-End Network Management Software", pages 1-6, Nov. 11, 1997", containing at least: Solstice Enterprise Manager is unique in that it provides the **distributed** multi-protocol management solution that can **manage networks with millions of objects** and ever-changing technologies, and enables providers to be first to market with differentiated services marked by visible quality. Solstice Enterprise Manager 2.1: -0- -- Builds on the power of the product's scalable and **distributed architecture,** by breaking out common management services into **distributed components**. For the first time, customers can distribute the logging, Simple Network Management Protocol, Common Management Information Protocol and Remote Procedure Call services as **separate processes in the network**. -- Liberates network administrators by allowing them to provide customers with **highly-secured access** to management information through new **object-level access control**. For example, an IT organization responsible for discreetly managing services available within both the engineering and finance organizations should keep these separate domains with **rights, privileges and access very carefully controlled**. **Secure management functionality** is built into Solstice Enterprise Manager. This can also be used by **ISPs spanning** commerce efforts across **multiple companies** (e.g., network management service provided to both Coke and Pepsi).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker-Lucent with the teachings of SUN in order to facilitate usage at individual object level because the concept of accessing individual object level would enhance supporting event / request by the object. The concept of accessing a single object would enhance supporting event / request for the particular object. The prevention of not accessing the other object when accessing the object would enhance supporting event / request specific to the object and not in common with the other object.

13. As per claims 5, 24 and 43, Barker-Lucent, Barry and SUN disclose the claimed limitations as rejected above. Barker-Lucent also teaches the following:

the events or requests are delivered by the gateway through the platform-independent interface according to Internet Inter-Object Protocol (IIOP) (e.g., use of IIOP protocol, col. 9, lines 15-19).

14. As per claims 6-7, 25-26 and 44-45, Barker-Lucent, SUN disclose the claimed limitations as rejected above. Barker-Lucent also teaches the following:

the platform-independent interface to the gateway is expressed in an interface definition language (e.g., use of interface description language (IDL), col. 39, lines 1-15, figure 15), and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages (e.g., IDL is used to describe any resource or service a server component wants to expose to its clients without regard to its implementation language or operating system, col. 39, lines 1-15, figure 15),

the interface definition language comprises OMG IDL (e.g., use of object management group (OMG) IDL, col. 7, lines 1-30).

15. As per claims 9, 28 and 47, Barker-Lucent, SUN disclose the claimed limitations as rejected above. Barker-Lucent also teaches the following:

the managed objects comprise an object corresponding to a telecommunications device (e.g., col., 2, line 49 – col., 3, line 40).

16. As per claims 16-17, 35-36 and 54-55, Barker-Lucent, SUN disclose the claimed limitations as rejected above. Barker-Lucent also teaches the following:

the requests comprise a query for information concerning the managed object (e.g., col. 40, lines 27-38),

the requests comprise a command to set parameter of the managed object (e.g., col. 40, lines 27-38).

17. Claims 8, 27, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, SUN in view of "Official Notice".

18. As per claims 8, 27 and 46, Barker-Lucent, SUN disclose the claimed limitations as rejected above. However, Barker-Lucent, SUN do not specifically mention about object corresponding to a telephone network. "Official Notice" is taken that both the concept and advantages of providing object corresponding to a telephone network is well known and expected in the art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include object corresponding to a telephone network with the teachings of Barker-Lucent, SUN in order to facilitate usage of object corresponding to a telephone network because the object corresponding to a telephone network would support information related to the telephone network. The gateway would help utilize the information.

19. Claims 2-4, 10, 21-23, 29, 40-42, 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, SUN in view of Olden, 6,460,141, RSA Security Inc., (Hereinafter Olden-RSA-Security).

20. As per claims 2-4, 21-23 and 40-42, Barker-Lucent, SUN disclose the claimed limitations as rejected above. Barker-Lucent also teaches the gateway is configurable to determine whether each of the managers can communicate with each of the managed objects, receive the events from the managed objects / managed object generating the event (e.g., col. 8, lines 31-54).

However, Barker-Lucent, SUN do not specifically mention about authorization as a function of the identity of the managed object / user Ids entered by users of the managers.

Olden-RSA-Security discloses the well-known concept of authorization (e.g., abstract) as a function of the identity of the managed object (e.g., col., 9, lines 2 – 34) / user IDs entered by users of the managers (e.g., col., 25, lines 5 – col., 26, line 28, col., 7, lines 31 - 57).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker-Lucent, SUN with the teachings of Olden-RSA-Security in order to facilitate authorization as a function of the identity of the managed object / user Ids entered by users of the managers because the authorization would enhance verifying that the managed object is been accessed by the valid manager and not the unauthorized manager. The User IDs of the users and the identity of the managed object would help support providing authorization functionality.

21. As per claims 10, 29 and 48, Barker-Lucent, SUN disclose the claimed limitations as rejected above. Barker-Lucent also teaches the gateway is configurable to provide audit trails (e.g., col., 17, line 27 – col., 18, line 67).

However, Barker-Lucent, SUN do not specifically mention about security information.

Olden-RSA-Security discloses the well-known concept of usage of security information (e.g., abstract, e.g., col., 29, lines 1 - 58).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker-Lucent, Barry and CORBA/TMN with the teachings of Olden-RSA-Security in order to facilitate usage of security because the security information would enhance keeping track of the activities that occur with the information related to handled objects. The audit information would be available in future.

22. Claims 11-15, 30-34 and 49-53, are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry, SUN in view of "Official Notice".

23. As per claims 11-15, 30-34 and 49-53, Barker-Lucent, SUN and Olden-RSA-Security disclose the claimed limitations as rejected above.

Barker-Lucent also teaches the gateway providing logging (e.g., col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53), to log user information that sends each request (e.g., col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53), to log information of the managed object that is the source of each event (e.g., col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53), to log a time at which each event is generated / delivered (e.g., col., 11, lines 18 – 60, col. 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53, col., 31, lines 15 – col., 43, col., 39, line 24 – col., 40, line 29, col., 23, line 55 – col., 24, line 10).

However, Barker-Lucent, SUN and Olden-RSA-Security do not specifically mention about providing access to a logging service, to log an ID of a user, to log an ID of the object.

"Official Notice" is taken that both the concept and advantages of providing access to a logging service, to log an ID of a user, to log an ID of the object is well known and expected in the art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include providing access to a logging service, to log an ID of a user, to log an ID of the object with the teachings of Barker-Lucent, SUN and Olden-RSA-Security in order to facilitate usage of access to a logging service, to log an ID of a user, to log an ID of the object because the accessing would enhance utilizing the logging service. The ID of the user and the object would help enhance logging information regarding the user and the object.

24. Claims 18, 37 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, SUN in view of Hearne et al., 2001/0052113 (Hereinafter Hearne) in view of Solstice Enterprise Manager 4.1 Managing your network, Chapter 1, 08/16/1998, pages 1-27, SUN2 (Hereinafter SUN2).

25. As per claims 18, 37 and 56, Barker-Lucent, SUN disclose the claimed limitations as rejected above.

Barker-Lucent also teaches the requests are converted from one format to another format prior to delivery to the managed objects (e.g., usage of CORBA, IDL/IIOP, etc., col., 21, line 46 – col., 22, line 59).

However, Barker-Lucent, SUN and Olden-RSA-Security do not specifically mention about conversion from the interface definition language to a platform-specific format.

Hearne discloses the well-known concept of conversion from the interface definition language to a platform-specific format (e.g., abstract, paragraph 58 – 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker-Lucent, SUN and Olden-RSA-Security with the teachings of Hearne in order to facilitate conversion from the interface definition language to a platform-specific format because the conversion would enhance supporting information in a platform-specific format. The converted information from the interface definition language would support communication between two entities.

However, Barker-Lucent, SUN, Olden-RSA-Security and Hearne do not specifically mention about Portable Management Interface (PMI).

SUN2 discloses the well-known usage of Portable Management Interface (PMI) (e.g., figure 1-1, page 5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker-Lucent, SUN, Olden-RSA-Security and Hearne with the teachings of SUN2 in order to facilitate usage of well-known usage of Portable Management Interface (PMI) because the platform-specific format being PMI would enhance the managed object to utilize the format structure of PMI for communication with another entity.

The object would benefit implementation of information using PMI format for sending event and/or receiving request.

26. Claims 19, 38 and 57, are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, SUN in view of Hearne et al., 2001/0052113 (Hereinafter Hearne).

27. As per claims 19, 38 and 57, Barker-Lucent, SUN disclose the claimed limitations as rejected above.

Barker-Lucent also teaches the requests are converted from one format to another format prior to delivery to the managed objects (e.g., usage of CORBA, IDL/IIOP, etc., col., 21, line 46 – col., 22, line 59).

However, Barker-Lucent, SUN and Olden-RSA-Security do not specifically mention about conversion from the interface definition language to a platform-specific format.

Hearne discloses the well-known concept of conversion from the interface definition language to a platform-specific format (e.g., abstract, paragraph 58 – 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Barker-Lucent, SUN and Olden-RSA-Security with the teachings of Hearne in order to facilitate conversion from the interface definition language to a platform-specific format because the conversion would enhance supporting information in a platform-specific format. The converted information from the interface definition language would support communication between two entities.

28. Claims 1, 5-7, 9, 16-17, 20, 24-26, 28, 35-36, 39, 43-45, 47, 54-55, 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki et al., 6,751,677, Hewlett Packard (Hereinafter Ilnicki-HP) in view of SUN.

29. As per claims 1, 20, 39, 58-60, Ilnichi-HP teaches (**explicit CORBA gateway with firewall,** etc, which the applicant indicated) the following: a network management method / a carrier medium/ system comprising (e.g., cols. 3, 4), a gateway (e.g., an element management server, cols. 3, 4) which is coupled to a plurality of managed objects (e.g. cols. 3, 4) and which is configured to deliver events generated by the managed objects to manager (e.g., cols. 3, 4) or to deliver requests generated by the managers to the managed object (e.g., cols. 3, 4); and a platform-independent interface to the gateway (e.g., cols. 3, 4), wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the events or requests (e.g., cols. 3, 4), wherein the gateway is configurable to provide object-level control (e.g., cols. 3, 4), between the managers (e.g., cols. 3, 4) and the managed objects (e.g., cols. 3, 4) to send the requests to the managed objects (e.g., cols. 3, 4), sending an identity of a user of a manager application to a gateway (e.g., cols. 3, 4), determine on a managed object level whether or not the manager application (e.g., cols. 3, 4) is allowed to receive an event generated by one of plurality of managed objects (e.g., cols. 3, 4) or to send a request to the one of the plurality of managed objects (e.g., cols. 3, 4) as a function of the identity of the user of the manager application (e.g., cols. 3, 4), whereby access for the manager application to send the request is approved or denied for said managed object (e.g., cols. 3, 4). delivering the event to the manager application or the request to the managed object if the manager access is approved (e.g., cols. 3, 4).

However, Ilnicki-HP does not specifically mention about individual object level.

SUN discloses the well-known concept of usage at individual object level, access control so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects access control so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects and the usage of a request Service Access Point (SAP), "Sun Launches New Version of its High-End Network Management Software", pages 1-6, Nov. 11, 1997", containing at least: Solstice Enterprise Manager is unique in that it provides the **distributed** multi-protocol management solution that can **manage networks with millions of objects** and ever-changing technologies, and enables providers to be first to market with differentiated services marked by visible quality. Solstice Enterprise Manager 2.1: -0- -- Builds on the power of the product's scalable and **distributed architecture,** by breaking out common management services into **distributed components**. For the first time, customers can distribute the logging, Simple Network Management Protocol, Common Management Information Protocol and Remote Procedure Call services as **separate processes in the network**. -- Liberates network administrators by allowing them to provide customers with **highly-secured access** to management information through new **object-level access control**. For example, an IT organization responsible for discreetly managing services available within both the engineering and finance organizations should keep these separate domains with **rights, privileges and access very carefully controlled**. **Secure management functionality** is built into Solstice Enterprise Manager. This can also be used by **ISPs spanning** commerce efforts across **multiple companies** (e.g., network management service provided to both Coke and Pepsi).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ilnicki-HP with the teachings of SUN in order to facilitate usage at individual object level because the concept of accessing individual object level would enhance supporting event / request by the object. The concept of accessing a single object would enhance supporting event / request for the particular object. The prevention of not accessing the other object when accessing the object would enhance supporting event / request specific to the object and not in common with the other object.

30. As per claims 5, 24 and 43, Ilnicki-HP, Barry and SUN disclose the claimed limitations as rejected above. Ilnicki-HP also teaches the following:

the events or requests are delivered by the gateway through the platform-independent interface according to Internet Inter-Object Protocol (IIOP) (e.g., cols., 5, 6).

31. As per claims 6-7, 25-26 and 44-45, Ilnicki-HP, SUN disclose the claimed limitations as rejected above. Ilnicki-HP also teaches the following:

the platform-independent interface to the gateway is expressed in an interface definition language (e.g., cols., 5, 6), and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages (e.g., cols., 5, 6),

the interface definition language comprises OMG IDL (e.g., cols., 5, 6).

32. As per claims 9, 28 and 47, Ilnicki-HP, SUN disclose the claimed limitations as rejected above. Ilnicki-HP also teaches the following:

the managed objects comprise an object corresponding to a telecommunications device (e.g., cols., 5, 6).

33. As per claims 16-17, 35-36 and 54-55, Ilnicki-HP, SUN disclose the claimed limitations as rejected above. Ilnicki-HP also teaches the following:

the requests comprise a query for information concerning the managed object (e.g., cols., 5, 6),

the requests comprise a command to set parameter of the managed object (e.g., cols., 5, 6).

34. Claims 8, 27, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki-HP, SUN in view of "Official Notice".

35. As per claims 8, 27 and 46, Ilnicki-HP, SUN disclose the claimed limitations as rejected above. However, Ilnicki-HP, SUN do not specifically mention about object corresponding to a telephone network. "Official Notice" is taken that both the concept and advantages of providing object corresponding to a telephone network is well known and expected in the art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include object corresponding to a telephone network with the teachings of Ilnicki-HP, SUN in order to facilitate usage of object corresponding to a telephone network because the object corresponding to a telephone network would support information related to the telephone network. The gateway would help utilize the information.

36. Claims 2-4, 10, 21-23, 29, 40-42, 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki-HP, SUN in view of Olden, 6,460,141, RSA Security Inc., (Hereinafter Olden-RSA-Security).

37. As per claims 2-4, 21-23 and 40-42, Ilnicki-HP, SUN disclose the claimed limitations as rejected above. Ilnicki-HP also teaches the gateway is configurable to determine whether each of the managers can communicate with each of the managed objects, receive the events from the managed objects / managed object generating the event (e.g., col. 8, lines 31-54).

However, Ilnicki-HP, SUN do not specifically mention about authorization as a function of the identity of the managed object / user Ids entered by users of the managers.

Olden-RSA-Security discloses the well-known concept of authorization (e.g., abstract) as a function of the identity of the managed object (e.g., col., 9, lines 2 – 34) / user IDs entered by users of the managers (e.g., col., 25, lines 5 – col., 26, line 28, col., 7, lines 31 - 57).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ilnicki-HP, SUN with the teachings of Olden-RSA-Security in order to facilitate authorization as a function of the identity of the managed object / user Ids entered by users of the managers because the authorization would enhance verifying that the managed object is been accessed by the valid manager and not the unauthorized manager. The User IDs of the users and the identity of the managed object would help support providing authorization functionality.

38. As per claims 10, 29 and 48, Ilnicki-HP, SUN disclose the claimed limitations as rejected above. Ilnicki-HP also teaches the gateway is configurable to provide audit trails (e.g., col., 17, line 27 – col., 18, line 67).

However, Ilnicki-HP, SUN do not specifically mention about security information.

Olden-RSA-Security discloses the well-known concept of usage of security information (e.g., abstract, e.g., col., 29, lines 1 - 58).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ilnicki-HP, Barry and CORBA/TMN with the teachings of Olden-RSA-Security in order to facilitate usage of security because the security information would enhance keeping track of the activities that occur with the information related to handled objects. The audit information would be available in future.

39. Claims 11-15, 30-34 and 49-53, are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki-HP, Barry, SUN in view of “Official Notice”.

40. As per claims 11-15, 30-34 and 49-53, Ilnicki-HP, SUN and Olden-RSA-Security disclose the claimed limitations as rejected above.

Ilnicki-HP also teaches the gateway providing logging (e.g., col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53), to log user information that sends each request (e.g., col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53), to log information of the managed object that is the source of each event (e.g., col., 11, lines 18 – 60, col., 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53), to log a time at which each event is generated / delivered (e.g., col., 11, lines 18 – 60, col. 17, line 33 – col., 18, line 9, col., 41, line 63 – col., 42, line 53, col., 31, lines 15 – col., 43, col., 39, line 24 – col., 40, line 29, col., 23, line 55 – col., 24, line 10).

However, Ilnicki-HP, SUN and Olden-RSA-Security do not specifically mention about providing access to a logging service, to log an ID of a user, to log an ID of the object.

“Official Notice” is taken that both the concept and advantages of providing access to a logging service, to log an ID of a user, to log an ID of the object is well known and expected in the art.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include providing access to a logging service, to log an ID of a user, to log an ID of the object with the teachings of Ilnicki-HP, SUN and Olden-RSA-Security in order to facilitate usage of access to a logging service, to log an ID of a user, to log an ID of the object because the accessing would enhance utilizing the logging service. The ID of the user and the object would help enhance logging information regarding the user and the object.

41. Claims 18, 37 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki-HP, SUN in view of Hearne et al., 2001/0052113 (Hereinafter Hearne) in view of Solstice Enterprise Manager 4.1 Managing your network, Chapter 1, 08/16/1998, pages 1-27, SUN2 (Hereinafter SUN2).

42. As per claims 18, 37 and 56, Ilnicki-HP, SUN disclose the claimed limitations as rejected above.

Ilnicki-HP also teaches the requests are converted from one format to another format prior to delivery to the managed objects (e.g., cols., 5, 6).

However, Ilnicki-HP, SUN and Olden-RSA-Security do not specifically mention about conversion from the interface definition language to a platform-specific format.

Hearne discloses the well-known concept of conversion from the interface definition language to a platform-specific format (e.g., abstract, paragraph 58 – 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ilnicki-HP, SUN and Olden-RSA-Security with the teachings of Hearne in order to facilitate conversion from the interface definition language to a platform-specific format because the conversion would enhance supporting information in a platform-specific format. The converted information from the interface definition language would support communication between two entities.

However, Ilnicki-HP, SUN, Olden-RSA-Security and Hearne do not specifically mention about Portable Management Interface (PMI).

SUN2 discloses the well-known usage of Portable Management Interface (PMI) (e.g., figure 1-1, page 5).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ilnicki-HP, SUN, Olden-RSA-Security and Hearne with the teachings of SUN2 in order to facilitate usage of well-known usage of Portable Management Interface (PMI) because the platform-specific format being PMI would enhance the managed object to utilize the format structure of PMI for communication with another entity. The object would benefit implementation of information using PMI format for sending event and/or receiving request.

43. Claims 19, 38 and 57, are rejected under 35 U.S.C. 103(a) as being unpatentable over Ilnicki-HP, SUN in view of Hearne et al., 2001/0052113 (Hereinafter Hearne).

44. As per claims 19, 38 and 57, Ilnicki-HP, SUN disclose the claimed limitations as rejected above.

Ilnicki-HP also teaches the requests are converted from one format to another format prior to delivery to the managed objects (e.g., cols., 5, 6).

However, Ilnicki-HP, SUN and Olden-RSA-Security do not specifically mention about conversion from the interface definition language to a platform-specific format.

Hearne discloses the well-known concept of conversion from the interface definition language to a platform-specific format (e.g., abstract, paragraph 58 – 62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ilnicki-HP, SUN and Olden-RSA-Security with the teachings of Hearne in order to facilitate conversion from the interface definition language to a platform-specific format because the conversion would enhance supporting information in a platform-specific format. The converted information from the interface definition language would support communication between two entities.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

45. Claims 1-6, 8-11, 16, 17, 20-25, 27-30, 35, 36, 39-44, 46-49, 54, 55, 58-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Sondur et al. 6,282,568, SUN Microsystems (Hereinafter Sondur-SUN-Microsystems).

46. As per claims 1, 20, 39, 58-60, Sondur-SUN Microsystems teaches (**explicit teachings of PMI + CORBA + Gateway + Solstice EM distributed network management system, etc.,** (the Solstice EM distributed network management system belongs to SUN Microsystems and the **characteristics of the Solstice** is also considered which are presented by the same assignee of this application): a network management method / a carrier medium/ system comprising (e.g., cols., 2, 3) a gateway which is coupled to a plurality of managed objects and which is configured to deliver events generated by the managed objects to manager (e.g., cols., 2, 3), or to deliver requests generated by the managers to the managed object (e.g., cols., 2, 3), and a platform-independent interface to the gateway (e.g., cols., 2, 3), wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the events or requests (e.g., cols., 2,3); wherein the gateway is configurable to provide object-level control (e.g., cols., 2, 3), between the managers and the managed objects to send the requests to the managed objects (e.g., cols., 2, 3), sending an identity of a user of a manager application to a gateway (e.g., cols., 2, 3), determine on a managed object level whether or not the manager application (e.g., cols., 2, 3), is allowed to receive an event generated by one of plurality of managed objects (e.g., cols., 2, 3), or to send a request to the one of the plurality of managed objects (e.g., cols., 2, 3), as a function of the identity of the user of the manager application (e.g.,

cols., 2, 3); whereby access for the manager application to send the request is approved or denied for said managed object (e.g., cols., 2, 3) and the usage of request SAP (e.g., cols., 2, 3), delivering the event to the manager application or the request to the managed object if the manager access is approved (e.g., cols., 2, 3), individual object level and access control (e.g., cols., 2, 3), so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects (e.g., cols., 2, 3).

47. As per claims 2-4, 21-23 and 40-42, Sondur-SUN Microsystems also teaches the following:

the gateway is configurable to determine whether each of the managers can communicate with each of the managed objects, receive the events from the managed objects / managed object generating the event (e.g., cols., 4, 5),

authorization as a function of the identity of the managed object / user Ids entered by users of the managers (e.g., cols., 4, 5).

48. As per claims 5, 24 and 43, Sondur-SUN Microsystems also teaches the following:

the events or requests are delivered by the gateway through the platform-independent interface according to Internet Inter-Object Protocol (IIOP) (e.g., cols., 4, 5).

49. As per claims 6, 25 and 44, Sondur-SUN Microsystems also teaches the following:

the platform-independent interface to the gateway is expressed in an interface definition language (e.g., cols., 4, 5); and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages (e.g., cols., 4, 5).

50. As per claims 8, 27, 46, Sondur-SUN Microsystems also teaches the following:

object corresponding to a telephone network (e.g., cols., 4, 5).

51. As per claims 9, 28 and 47, Sondur-SUN Microsystems also teaches the following:

the managed objects comprise an object corresponding to a telecommunications device (e.g., cols., 7, 8).

52. As per claims 10, 29 and 48, Sondur-SUN Microsystems also teaches the following:

the gateway is configurable to provide audit trails and security information (e.g., cols., 7, 8).

53. As per claims 11, 30 and 49, Sondur-SUN Microsystems also teaches the following:

the gateway providing access to a logging service (e.g., cols., 7, 8).

54. As per claims 16-17, 35-36 and 54-55, Sondur-SUN Microsystems also teaches the following:

the requests comprise a query for information concerning the managed object (e.g., cols., 7, 8), the requests comprise a command to set parameter of the managed object (e.g., cols., 7, 8).

55. Claims 1-6, 8-11, 16, 17, 20-25, 27-30, 35, 36, 39-44, 46-49, 54, 55, 58-60 are rejected under 35 U.S.C. 102(e) as being anticipated by Sondur et al. 6,282,568, SUN Microsystems (Hereinafter Sondur-SUN-Microsystems).

56. As per claims 1, 20, 39, 58-60, Rangrajan-SUN-Microsystems teaches (**explicit teachings of PMI + CORBA + Gateway + Solstice EM distributed network management system, etc.,** (the Solstice EM distributed network management system belongs to SUN Microsystems and the **characteristics of the Solstice** is also considered which are presented by the same assignee of this application): a network management method / a carrier medium/ system comprising (e.g., cols., 3, 4) a gateway which is coupled to a plurality of managed objects and which is configured to deliver events generated by the managed objects to manager (e.g., cols., 3, 4), or to deliver requests generated by the managers to the managed object (e.g., cols., 3, 4), and a platform-independent interface to the gateway (e.g., cols., 3, 4), wherein the gateway is configurable to communicate with the managers through the platform-independent interface to deliver the events or requests (e.g., cols., 3, 4); wherein the gateway is configurable to provide object-level control (e.g., cols., 3, 4), between the managers and the managed objects to send the requests to the managed objects (e.g., cols., 3, 4), sending an identity of a user of a manager application to a gateway (e.g., cols., 3, 4), determine on a managed object level whether or not the manager application (e.g., cols., 3, 4), is allowed to receive an event generated by one of plurality of managed objects (e.g., cols., 3, 4), or to send a request to the one of the plurality of

managed objects (e.g., cols., 3, 4), as a function of the identity of the user of the manager application (e.g., cols., 3, 4); whereby access for the manager application to send the request is approved or denied for said managed object (e.g., cols., 3, 4) and the usage of request SAP (e.g., cols., 3, 4), delivering the event to the manager application or the request to the managed object if the manager access is approved (e.g., cols., 3, 4), individual object level and access control (e.g., cols., 3, 4), so that one of the managers is granted access to one of the managed objects while being prevented from interfacing with a different one of the managed objects (e.g., cols., 3, 4).

57. As per claims 2-4, 21-23 and 40-42, Rangrajan-SUN-Microsystems also teaches the following:

the gateway is configurable to determine whether each of the managers can communicate with each of the managed objects, receive the events from the managed objects / managed object generating the event (e.g., cols., 4, 5),

authorization as a function of the identity of the managed object / user Ids entered by users of the managers (e.g., cols., 4, 5).

58. As per claims 5, 24 and 43, Rangrajan-SUN-Microsystems also teaches the following:

the events or requests are delivered by the gateway through the platform-independent interface according to Internet Inter-Object Protocol (IIOP) (e.g., cols., 4, 5).

59. As per claims 6, 25 and 44, Rangrajan-SUN-Microsystems also teaches the following:

the platform-independent interface to the gateway is expressed in an interface definition language (e.g., cols., 4, 5); and wherein the interface definition language comprises a language for defining interfaces to the managed objects across a plurality of platforms and across a plurality of programming languages (e.g., cols., 4, 5).

60. As per claims 8, 27, 46, Rangrajan-SUN-Microsystems also teaches the following:

object corresponding to a telephone network (e.g., cols., 4, 5).

61. As per claims 9, 28 and 47, Rangrajan-SUN-Microsystems also teaches the following:

the managed objects comprise an object corresponding to a telecommunications device (e.g., cols., 7, 8).

62. As per claims 10, 29 and 48, Rangrajan-SUN-Microsystems also teaches the following:

the gateway is configurable to provide audit trails and security information (e.g., cols., 7, 8).

63. As per claims 11, 30 and 49, Rangrajan-SUN-Microsystems also teaches the following:

the gateway providing access to a logging service (e.g., cols., 7, 8).

64. As per claims 16-17, 35-36 and 54-55, Rangrajan-SUN-Microsystems also teaches the following:

the requests comprise a query for information concerning the managed object (e.g., cols., 7, 8),

the requests comprise a command to set parameter of the managed object (e.g., cols., 7, 8).

65. Claims 1, 5-7, 9, 16-17, 20, 24-26, 28, 35-36, 39, 43-45, 47, 54-55, 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent et al. U.S. patent number 6,363,421, Lucent Technologies (Hereinafter Barker-Lucent) in view of Barry et al., 6,615,258 (Hereinafter Barry) and JIDM Interaction Translation, Initial Submission to OMG's CORBA/TMN Internetworking RFP, Edition, 4.0, February 1998, pages, i-v, 1-1 to 7-132, 9-167 to 9-169 (Hereinafter CORBA/TMN), as per office action dated 6/18/2007.

66. Claims 8, 27, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and CORBA/TMN in view of "Official Notice" , as per office action dated 6/18/2007.

67. Claims 2-4, 10, 21-23, 29, 40-42, 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and CORBA/TMN in view of Olden, 6,460,141, RSA Security Inc., (Hereinafter Olden-RSA-Security) , as per office action dated 6/18/2007.

68. Claims 11-15, 30-34 and 49-53, are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry, CORBA/TMN and Olden-RSA-Security in view of "Official Notice" , as per office action dated 6/18/2007.

69. Claims 18, 37 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and CORBA/TMN in view of Hearne et al., 2001/0052113 (Hereinafter Hearne) in view of Solstice Enterprise Manager 4.1 Managing your network, Chapter 1, 08/16/1998, pages 1-27, SUN (Hereinafter SUN) , as per office action dated 6/18/2007.

70. Claims 19, 38 and 57, are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and CORBA/TMN in view of Hearne et al., 2001/0052113 (Hereinafter Hearne) , as per office action dated 6/18/2007.

71. Claims 1, 5-7, 9, 16-17, 20, 24-26, 28, 35-36, 39, 43-45, 47, 54-55, 58-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent in view of Barry et al., 6,615,258 (Hereinafter Barry) and Buckle et al., (Hereinafter Buckle) , as per office action dated 6/18/2007.

72. Claims 8, 27, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and Buckle in view of "Official Notice" , as per office action dated 6/18/2007.

73. Claims 2-4, 10, 21-23, 29, 40-42, 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and Buckle in view of Olden, 6,460,141, RSA Security Inc., (Hereinafter Olden-RSA-Security) , as per office action dated 6/18/2007.

74. Claims 11-15, 30-34 and 49-53, are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry, Buckle and Olden-RSA-Security in view of "Official Notice" , as per office action dated 6/18/2007.

75. Claims 18, 37 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and Buckle in view of Hearne et al., 2001/0052113 (Hereinafter Hearne) in

view of Solstice Enterprise Manager 4.1 Managing your network, Chapter 1, 08/16/1998, pages 1-27, SUN (Hereinafter SUN) , as per office action dated 6/18/2007.

76. Claims 19, 38 and 57, are rejected under 35 U.S.C. 103(a) as being unpatentable over Barker-Lucent, Barry and Buckle in view of Hearne et al., 2001/0052113 (Hereinafter Hearne) , as per office action dated 6/18/2007.

Response to Arguments

77. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection which clearly demonstrate applicant concerned "**Object level access control**". Regarding the rejections under 35 U.S.C. 103(a), Barker-Lucent et al. U.S. patent number 6,363,421, Lucent Technologies (Hereinafter Barker-Lucent), etc., please refer to the responses and rejections of the prosecution history, 2/22/2008, 11/28/2007, 6/18/2006, 10/05/2006, etc.

Allowable Subject Matter

78. Claims 61-63 are allowed. Applicant is encouraged to claim dependent claims 2-19 under claim 61, and other respective dependent claims under claims 62 and 63 (combination of subject matter of claims 61 or 62 or 63 with respective dependent claims) being one of the option for the applicant's benefit, see prosecution history.

Conclusion

Considering the long prosecution of this case, in order to expedite the prosecution of this case, multiple references are used for the rejections to demonstrate that several references disclose the claimed subject matter of the claims, including the applicant very concerned, "object level access control" – even word by word was published by the same assignee, Sun Micro Systems, at least more than one year before the filling of this application (1997), which is supported by the evidence as mentioned in the office action.

Examiner has cited particular columns and line numbers and/or paragraphs and/or sections and/or page numbers in the reference(s) as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety, as potentially teaching, all or part of the claimed invention, as well as the context of the passage, as taught by the prior art or disclosed by the Examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Haresh Patel whose telephone number is (571) 272-3973. The examiner can normally be reached on Monday, Tuesday, Thursday and Friday from 10:00 am to 8:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn, can be reached at (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Haresh N. Patel/

Primary Examiner, Art Unit 2154

6/6/2008